

Нормативно-правовое обеспечение кибербезопасности

План лекции

УЧЕБНЫЕ ВОПРОСЫ :

1. Задача нормативно-правового регулирования обеспечения кибербезопасности в Российской Федерации.

2. Законодательство Российской Федерации в области защиты информации.

План лекции

УЧЕБНЫЕ ВОПРОСЫ :

- 3. Основы государственной политики Российской Федерации в области международной информационной безопасности.*
- 4. Международные стандарты в области обеспечения кибербезопасности*

ЛИТЕРАТУРА

Нормативно-правовые акты, официальные издания

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 года.

2. О государственной тайне : закон РФ от 21 июля 1993 г. № 5485-1.

3. Об информации, информационных технологиях и о защите информации : федеральный закон от 27.07.2006 № 149-ФЗ/

ЛИТЕРАТУРА

Нормативно-правовые акты, официальные издания

4. О безопасности : федеральный закон от 28.12.2010 № 390-ФЗ //.

5. О безопасности критической информационной инфраструктуры Российской Федерации : федеральный закон от 26 июля 2017 г. № 187-ФЗ.

6. О связи: федеральный закон от 7 июля 2003 г. № 126-ФЗ.

7. О полиции : федеральный закон от 7 февраля 2011 № 3-ФЗ.

ЛИТЕРАТУРА

Нормативно-правовые акты, официальные издания

8. Об электронной подписи : федеральный закон от 06.04.2011 № 63-ФЗ.

9. О персональных данных: федеральный закон от 27.07.2006 №152-ФЗ.

10. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.

11. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 г. № 195-ФЗ

ЛИТЕРАТУРА

Нормативно-правовые акты, официальные издания

12. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 5 декабря 2016 года № 646.

13. О Стратегии национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 2 июля 2021 года № 400.

ЛИТЕРАТУРА

Нормативно-правовые акты, официальные издания

14. Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности : Указ Президента Российской Федерации от 12 апреля 2021 г. № 213.

15. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» : приказ ФСТЭК России от 25 декабря 2017 г. № 239.

ЛИТЕРАТУРА

Основная литература

1. **Основы информационной безопасности** : учебник / **В. Ю. Рогозин**, И. Б. Галушкин, В.К. Новиков, С.Б. Вепрев ; Академия Следственного комитета Российской Федерации. – **Москва** : ЮНИТИ-ДАНА, **2019**. – 287 с..

2. **Основы информационной безопасности в органах внутренних дел** : учеб. пособие / сост. **А.Б. Сизоненко**, С.Г. Ключев, В.Н. Цимбал. - **Краснодар** : Краснодарский университет МВД России, **2016**. – 122 с..

ЛИТЕРАТУРА

Основная литература

3. Костюченко, К.Л. **Основы информационной безопасности в органах внутренних дел** : учеб. пособие / К. Л. Костюченко, С. В. Мухачев. – Екатеринбург: Уральский юридический институт МВД России, **2015**.

1. Задача нормативно-правового регулирования обеспечения кибербезопасности в Российской Федерации.

Стратегия национальной безопасности Российской Федерации

(утверждена Указом Президента РФ от
02.07.2021 N 400)

базовый документ планирования,
определяющий:

- **национальные интересы и приоритеты России;**
- **цели и задачи государственной политики в области обеспечения национальной безопасности и устойчивого развития страны на долгосрочную перспективу.**

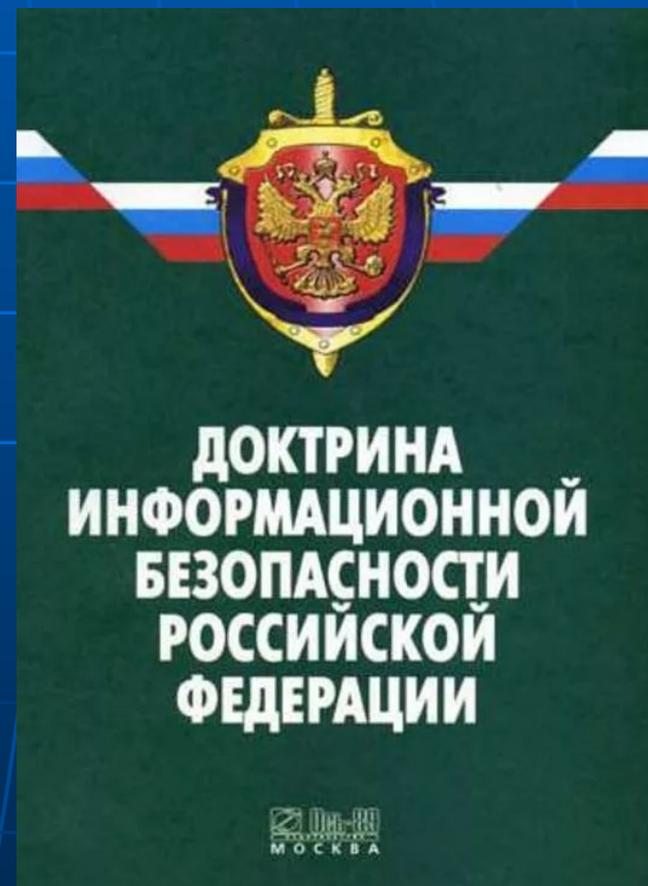
Стратегические национальные приоритеты:

- 1) сбережение народа России и развитие человеческого потенциала;
- 2) оборона страны;
- 3) государственная и общественная безопасность;
- 4) информационная безопасность;
- 5) экономическая безопасность;
- 6) научно-технологическое развитие;
- 7) экологическая безопасность и рациональное природопользование;
- 8) защита традиционных российских духовно-нравственных ценностей, культуры и исторической памяти;
- 9) стратегическая стабильность и взаимовыгодное международное сотрудничество.

Основа для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности —

**Доктрина
информационной
безопасности
Российской Федерации**

**(утверждена указом
Президента РФ
05.12.2016 № 646)**



Принципы государственной политики обеспечения информационной безопасности:

- **законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений**, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;
- **конструктивное взаимодействие** государственных органов, организаций и граждан **при решении задач** по обеспечению информационной безопасности;

Принципы государственной политики обеспечения информационной безопасности:

- **соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями**, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;
- **достаточность сил и средств обеспечения информационной безопасности**, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

Принципы государственной политики обеспечения информационной безопасности:

- **соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.**

Национальные интересы в информационной сфере

- **обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;**

Национальные интересы в информационной сфере

- **обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры**, в первую очередь критической информационной инфраструктуры Российской Федерации, **и единой сети электросвязи Российской Федерации**, в мирное время, в период непосредственной угрозы агрессии и в военное время;

Национальные интересы в информационной сфере

- **развитие** в Российской Федерации **отрасли информационных технологий и электронной промышленности**, а также **совершенствование деятельности** производственных, научных и научно-технических организаций **по разработке, производству и эксплуатации средств обеспечения информационной безопасности**, оказанию услуг в области обеспечения информационной безопасности;

Национальные интересы в информационной сфере

- **доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;**

Национальные интересы в информационной сфере

- **содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.**

Государственные органы РФ,
контролирующие деятельность в области
защиты информации

Совет Безопасности России



**Государственные органы РФ,
контролирующие деятельность в области
защиты информации**

**Федеральная служба по техническому и
экспортному контролю
(ФСТЭК России)**



**является головным органом по защите
информации**

**Государственные органы РФ,
контролирующие деятельность в области
защиты информации**

**Федеральная служба безопасности
Российской Федерации
(ФСБ России)**



**Государственные органы РФ,
контролирующие деятельность в области
защиты информации**

**Федеральная служба охраны
(ФСО России)**



Государственные органы РФ, контролирующие деятельность в области защиты информации

Межведомственная комиссия по защите государственной тайны



Государство в процессе реализации своих функций по обеспечению ИБ:

- проводит объективный и всесторонний анализ и прогнозирование угроз ИБ РФ;**
- организует работу законодательных и исполнительных органов государственной власти РФ по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз ИБ;**

- **поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;**
- **осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;**

- **проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории РФ и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;**

- ***способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;***
- ***формулирует и реализует государственную информационную политику России.***

НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИБ

ПРАВОВАЯ
ЗАЩИТА

ОРГАНИЗАЦИОННАЯ
ЗАЩИТА

ИНЖЕНЕРНО-
ТЕХНИЧЕСКАЯ
ЗАЩИТА

ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ

- это специальные правовые акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе

МЕЖДУНАРОДНОЕ ПРАВО

- Договоры,
- Конвенции,
- Декларации,
- Патенты,
- Авторские права,
- Лицензии.

ВНУТРИГОСУДАРСТВЕННОЕ ПРАВО

Государственные

- Конституция,
- Законы (кодексы),
- Указы,
- Постановления.

Ведомственные

- Приказы,
- Руководства,
- Положения,
- Инструкции

ОРГАНИЗАЦИОННАЯ ЗАЩИТА

— это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.



ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА

— это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

ФИЗИЧЕСКИЕ

АППАРАТНЫЕ

ПРОГРАММНЫЕ

КРИПТОГРАФИЧЕСКИЕ

КОМБИНИРОВАННЫЕ

2. Законодательство Российской Федерации в области защиты информации.

Иерархия НПА в области защиты информации:

Конституция РФ

Федеральные законы

Указы Президента РФ

Постановления Правительства РФ

Приказы ФСБ России, ФСТЭК России,
Роскомнадзора

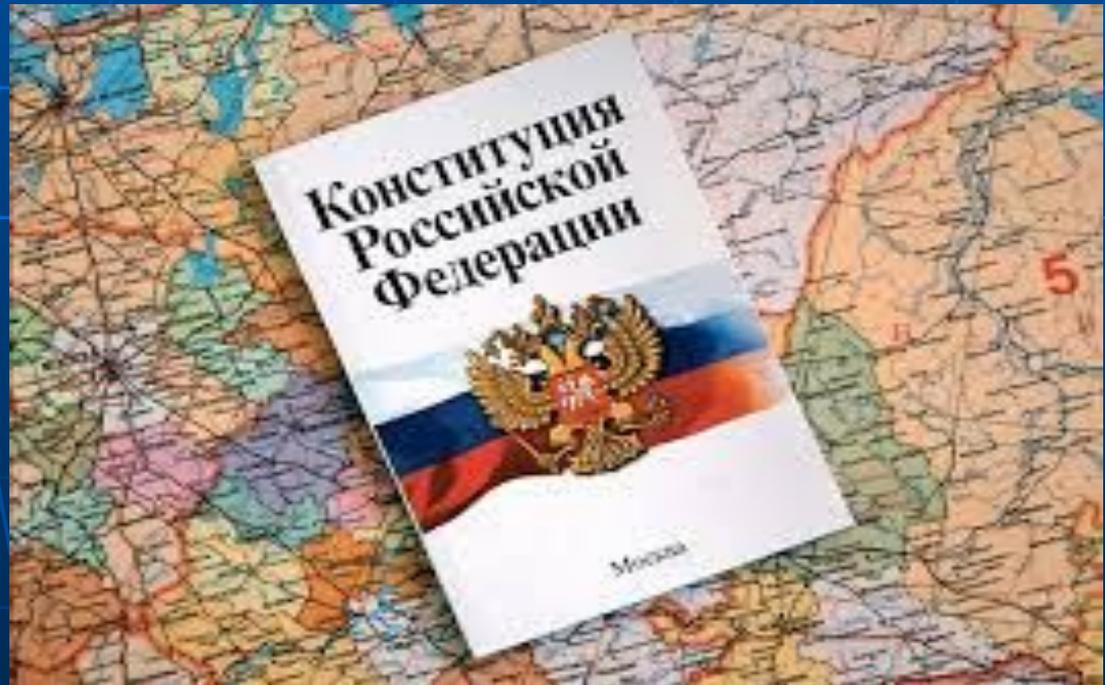
Стандарты, ГОСТы, методические документы
(носящие рекомендательный характер)

Внутренние организационно-распорядительные
документы (локальные акты организации)

Конституция РФ:

Основные статьи Конституции, которые прямо или косвенно определяют требования по информационной безопасности (защите информации)

- **ст. 23;**
- **ст. 24;**
- **ст. 29. п. 4.**



**Федеральный закон
от 28 декабря 2010 г. № 390-ФЗ
«О безопасности»**



Определяет ключевые термины в области безопасности, которые применимы и для сферы информационной безопасности, принципы и систему безопасности, правовой статус и состав Совета Безопасности Российской Федерации.

**Федеральный закон
от 27 июля 2006 г. № 149-ФЗ
«Об информации,
информационных технологиях
и защите информации»**



Фиксирует базовые нормы для всей системы информационного законодательства, в т.ч. правового обеспечения информационной безопасности.

Закон Российской Федерации от 21.07.1993 г. № 5485-1 «О государственной тайне»



Регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

Регулирует отношения,
связанные с обработкой
персональных данных
... с использованием
средств автоматизации,
в том числе в
информационно-
телекоммуникационных
сетях, или без
использования таких
средств...



Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»

Регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.



Федеральный закон от 26 июля 2017 г. N 187-ФЗ

«О безопасности критической информационной инфраструктуры Российской Федерации»

Регулирует отношения в области обеспечения
безопасности критической информационной

инфраструктуры РФ в
целях ее устойчивого
функционирования при
проведении в
отношении ее
компьютерных атак.



Уголовный кодекс РФ

(Федеральный закон от 13 июня 1996 г. № 63-ФЗ)



Предусматривает
уголовную
ответственность за
нарушение
установленных запретов
в информационной сфере

(более 50 отдельных статей) , в том числе за совершение преступлений в сфере компьютерной информации (ст.272, 273, 274, 274.1).

Кодекс РФ об административных правонарушениях (от 30 декабря 2001 г. № 195-ФЗ)

Определяет административную ответственность за правонарушения в области связи и информации (глава 13, ст. 13.1-13.24), а также за совершение иных проступков информационного характера (более 90 статей).



Иные ФЗ, в которых имеются статьи, определяющие и регулирующие отношения в области защиты информации:

- **от 27 декабря 2002 г. № 184-ФЗ**
«О техническом регулировании»
- **от 4 мая 2011 г. № 99-ФЗ**
«О лицензировании отдельных видов деятельности»
- **от 19 декабря 2005 г. № 160-ФЗ**
«О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке данных»

Иные ФЗ, в которых имеются статьи, определяющие и регулирующие отношения в области защиты информации:

- **от 3 апреля 1995 г. № 40-ФЗ**
«О Федеральной службе безопасности»
- **от 3 апреля 2008 г. № 294-ФЗ**
«О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»
- **от 6 апреля 2011 г. № 63-ФЗ**
«Об электронной подписи»

**Иные ФЗ, в которых имеются статьи,
определяющие и регулирующие отношения в
области защиты информации:**

- от 30 декабря 2001 г. № 197-ФЗ

Трудовой кодекс РФ

- от 26 января 1996 г. № 14-ФЗ

Гражданский кодекс РФ

Указы Президента РФ в области защиты информации

- **от 2 июля 2021 года № 400**
«О Стратегии национальной безопасности Российской Федерации»
- **от 5 декабря 2016 года № 646**
«Об утверждении Доктрины информационной безопасности Российской Федерации»
- **от 6 марта 1997 г. № 188**
«Об утверждении перечня сведений конфиденциального характера»

Указы Президента РФ в области защиты информации

- **от 30 ноября 1995 г. № 1203**
«Об утверждении Перечня сведений, отнесенных к государственной тайне»
- **от 6 октября 2004 г. № 1286**
«Вопросы Межведомственной комиссии по защите государственной тайны»
- **от 16 августа 2004 г. № 1085**
«Вопросы Федеральной службы по техническому и экспертному контролю»

Указы Президента РФ в области защиты информации

- от 11 августа 2003 г. № 960

«Об утверждении положения о Федеральной службе безопасности Российской Федерации и ее структуры»

- от 30 мая 2005 г. № 609

«Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»

Постановления Правительства в области защиты информации

- от 5 декабря 1991 г. №35

«О перечне сведений, которые не могут составлять коммерческую тайну»

- от 3 ноября 1994 г. № 1233

«Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии»

Постановления Правительства в области защиты информации

- **от 15 апреля 1995 г. № 333**

«Об утверждении Положения о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»

Постановления Правительства в области защиты информации

- **от 26 июня 1995 г. № 608**

«Об утверждении Положения о сертификации средств защиты информации»

- **от 4 сентября 1995 г. № 870**

«Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности»

Постановления Правительства в области защиты информации

- **от 15 сентября 2008 г. № 687**
«Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации»
- **от 6 февраля 2010 г. № 63**
«Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне»

Постановления Правительства в области защиты информации

- **от 21 ноября 2011 г. № 957**
«Об организации лицензирования отдельных видов деятельности»
- **от 3 февраля 2012 г. №79**
«О лицензировании деятельности по технической защите конфиденциальной информации»

и т.д.

В развитие и во исполнение Конституции РФ, Федеральных конституционных законов, Федеральных законов, указов Президента РФ, постановлений Правительства РФ **федеральные органы исполнительной власти** (ФСБ России, ФСТЭК России, Роскомнадзор) **издают нормативные правовые акты в виде постановлений, приказов, распоряжений, правил, инструкций и положений,** зарегистрированных в Минюсте России.

***3. Основы государственной политики
Российской Федерации в области
международной информационной
безопасности***

«Основы государственной политики Российской Федерации в области международной информационной безопасности»

утверждены
Указом Президента
Российской
Федерации
от 12 апреля 2021 г.
№ 213.

(далее Основы)



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Об утверждении Основ государственной политики
Российской Федерации в области международной
информационной безопасности

В целях обеспечения реализации государственной политики Российской Федерации в области международной информационной безопасности постановляю:

1. Утвердить прилагаемые Основы государственной политики Российской Федерации в области международной информационной безопасности.
2. Настоящий Указ вступает в силу со дня его подписания.



Президент
Российской Федерации В.Путин

Москва, Кремль
12 апреля 2021 года
№ 213

Основы направлены на:

- **продвижение** на международной арене **российских подходов к формированию системы обеспечения международной ИБ** и **российских инициатив в области международной ИБ;**
- **содействие созданию** международно-правовых **механизмов предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве;**
- **организацию межведомственного взаимодействия при реализации государственной политики в области международной ИБ.**

Основы являются документом стратегического планирования РФ

отражают

- официальные взгляды на сущность международной ИБ;

определяют:

- основные угрозы международной ИБ;
- цель и задачи государственной политики РФ в области международной ИБ;
- основные направления реализации государственной политики РФ в области международной ИБ.

Цель государственной политики в области международной ИБ:

- **содействие установлению международно-правового режима, при котором создаются условия для предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве;**
- **формирование системы обеспечения международной ИБ с учетом национальных интересов Российской Федерации.**

Основные угрозы международной ИБ:

- **использование ИКТ** в военно-политической и иных сферах **в целях подрыва суверенитета**, нарушения территориальной целостности государств, **осуществления** в глобальном информационном пространстве **иных действий, препятствующих поддержанию международного мира, безопасности и стабильности;**
- **использование ИКТ в террористических целях**, в том числе для пропаганды терроризма и привлечения к террористической деятельности **новых сторонников;**

Основные угрозы международной ИБ:

- использование ИКТ в экстремистских целях, а также для вмешательства во внутренние дела суверенных государств;
- использование ИКТ в преступных целях, в том числе для совершения преступлений в сфере компьютерной информации, а также для совершения различных видов мошенничества;
- использование ИКТ для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру;

Основные угрозы международной ИБ:

- использование отдельными государствами технологического доминирования в глобальном информационном пространстве для монополизации рынка информационно-коммуникационных технологий, ограничения доступа других государств к передовым информационно-коммуникационным технологиям, а также для усиления их технологической зависимости от доминирующих в сфере информатизации государств и информационного неравенства.

4. Международные стандарты в области обеспечения кибербезопасности

Изучение лучших практик дает возможность узнать:

- терминологию в сфере кибербезопасности;**
- общие подходы к построению кибербезопасности;**
- общепринятые процессы и рекомендации по их выстраиванию;**
- конкретные меры защиты.**

Типы стандартов

- **технические или контрольные (control)**, регламентирующие различные аспекты реализации мер защиты;
- **процессно-ориентированные**, описывающие подход к выстраиванию процессов и построению кибербезопасности в целом.

Обзор стандартов:

• **COBIT;**

• **ITIL и ITSM;**

• **ISO.**

